Get Memory
win32dd.exe /f infected.dmp
or
win64.dd

Analyze using volatility

python vol.py -f infected.dmp connections
python vol.py -f infected.dmp psscan
python vol.py -f infected.dmp handles -p pid -t Process
python vol.py -f infected.dmp apihooks -p pid
python vol.py -f infected.dmp volshell
    cc(pid=pidnumber)
look for jumps, use db with offset to look for PE (executable)
python vol.py -f infected.dmp vaddump -p PID -D wheretodumpexe

psinfo -h -s -d
netstat -
date
pslist
psservice
psfile

at

userdump suspiciousprocess location\for\dump
dumpchk dumpdadatefile

ntlast
psloglist

wmic computersystem get username
wmic service get name
wmic diskdrive get interfacetype
wmic nic get name
wmic nicconfig get ipaddress,macaddress
wmic logicaldisk get description,filesystem,name,size
wmic volume get label,freespace,filesystem,capacity,driveletter
wmic netlogin get name,badpasswordcount
wmic logon get authenticationpackage
wmic netclient get name

wmic netuse get name,username,connectiontype,localname
wmic netuse get name,username,connectiontype,localname
wmic share get name,path
wmic nteventlog get path,filename,writeable
wmic service get name,startmode,state,status
wmic os get name,servicepackmajorversion
wmic product get name,version

use filelist to get timestamps
http://www.jam-software.de/filelist/